Distributed Denial of Service Attacks

NITIN BISHT
140231
CSE III

Table of Content

- Introduction to DDoS
- How it Works
- Aim of DDoS Attack
- Types of DDoS
- DDoS Symptoms
- DDoS Mitigation
- Famous DDoS Attacks

Introduction

- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

- In the United States, the people that take part in DDoS attacks are charged with legal offenses at the federal level, both criminally and civilly.

Introduction

- The average DDoS attack is about 50 gbps.
- DDoS Duration :- not defined
- Targets :- Gaming industries , banks , news websites

DDoS VS DoS

- In a DoS attack, a hacker uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources .

- On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet.

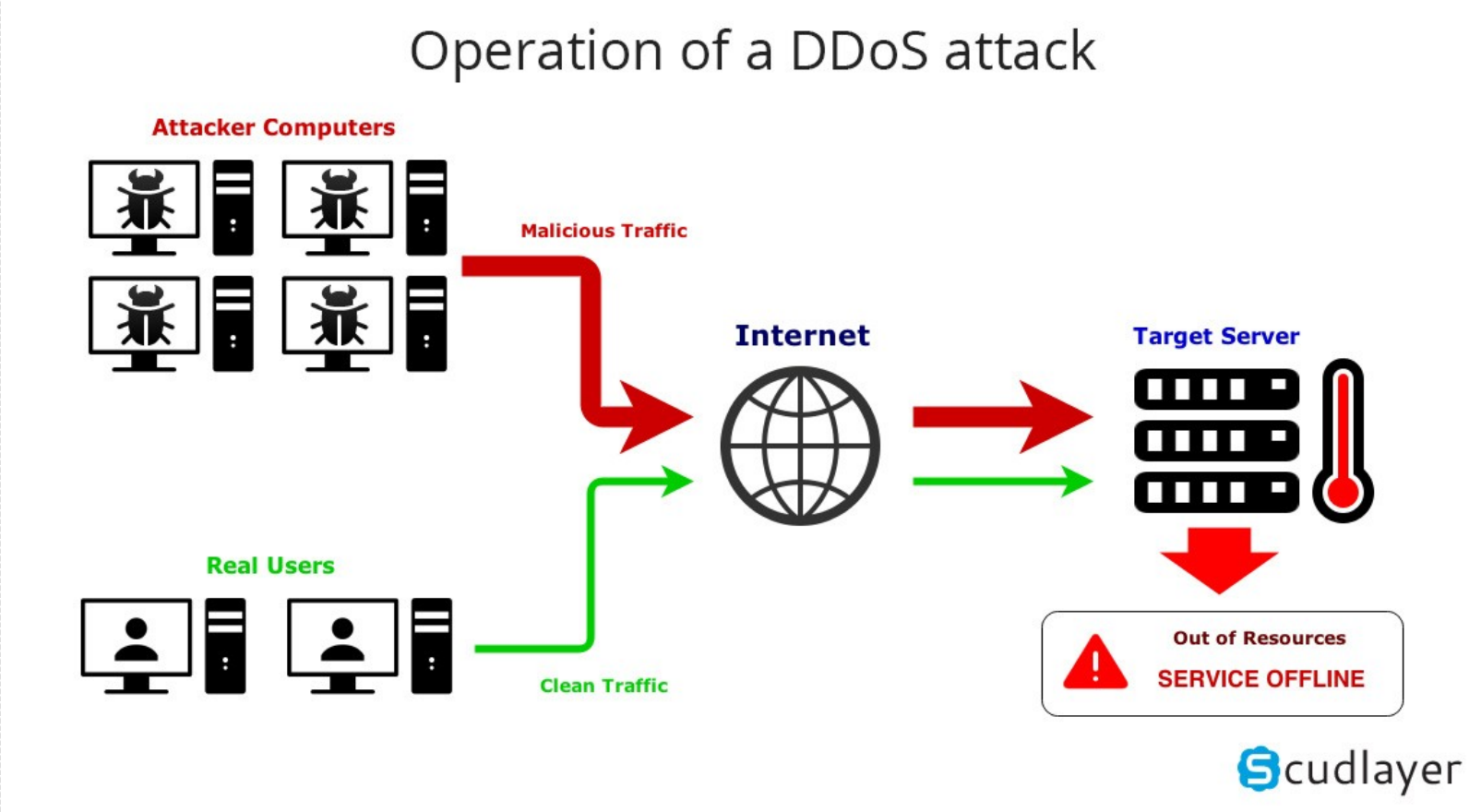
How DDoS attack works

- In a typical DDoS attack, the hacker begins by exploiting a computer system and making it the DDoS master.
- The attack master system identifies other vulnerable systems and gains control over them by either infecting the systems with malware or through bypassing the authentication controls .

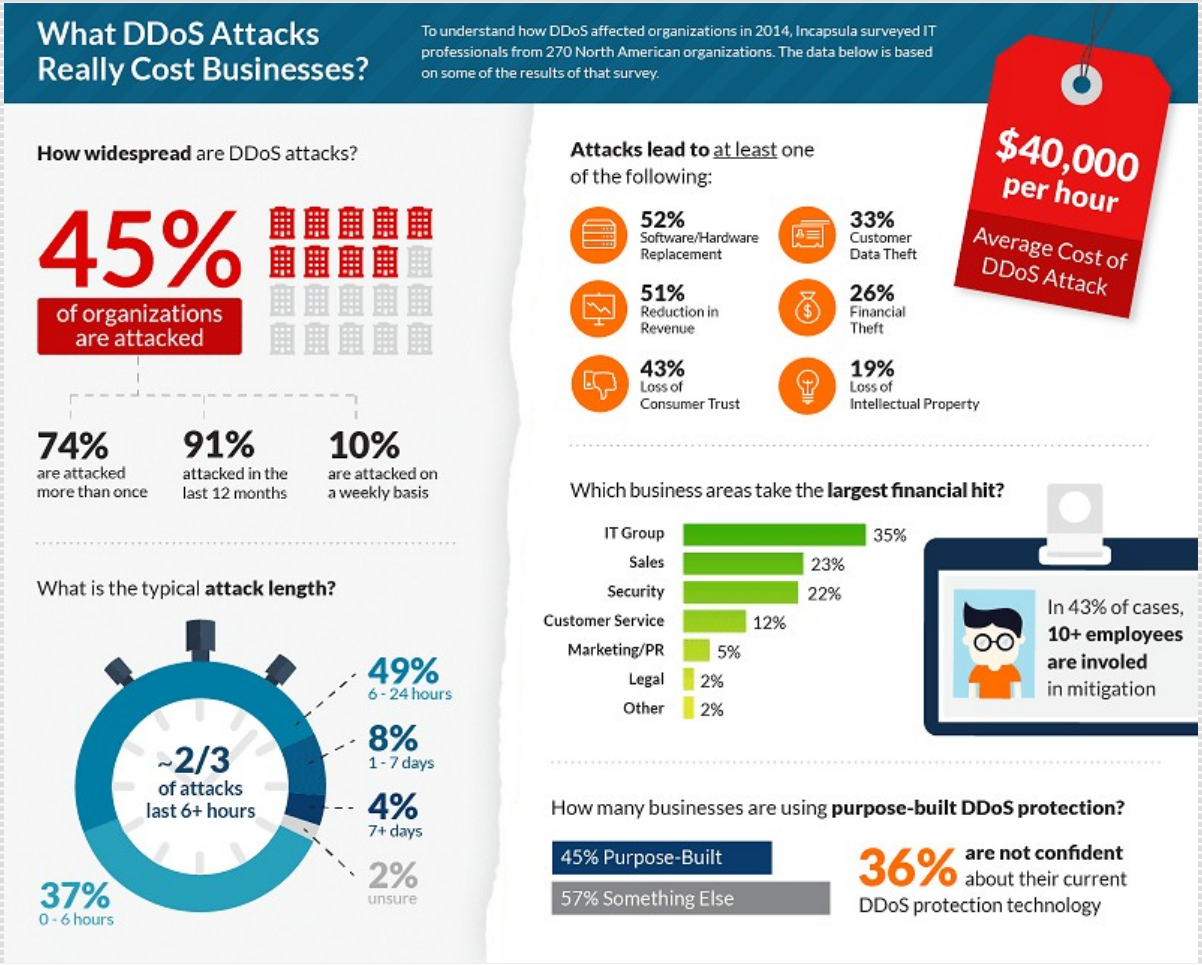
How DDoS attack works

- The attacker creates a command-and-control server to command the network of bots, also called a botnet.
- The person in control of a botnet is sometimes referred to as the botmaster.
- Their main aim is to prevent legitimate users from accessing a system or site.

DDoS attack


Operation of a DDoS attack
Attacker Computers
Malicious Traffic
Internet
Target Server
Real Users
Clean Traffic
Out of Resources
SERVICE OFFLINE
Scudlayer

DDoS Attack Report



AIM OF A DDoS ATTACK

Common reason for DDoS attacks are:

1. Expression of anger and criticism.
2. Training ground for other attacks.
3. Distraction from other malicious actions.
4. Anticompetitive business practices.
5. Means to extract money.
6. To disrupt operation of private or government enterprise.

Types of DDoS attacks

There are broadly 3 types of DDoS attacks :-

Network or Volume centric attack – 64%

Protocol attacks – 20%

Application layer attack - 16%

Network or Volume Centric

- These attacks use bots and botnets to flood the network layers with a substantial amount of seemingly legitimate traffic.

- This consumes an excessive amount of bandwidth within or outside of the network and causes network operations to become extremely slow or to not work at all.

Network or Volume Centric

- These kinds of attacks are more difficult to mitigate than attacks from a single source

- Volumetric attacks come in a variety of forms, including:

- User Datagram Protocol (UDP) Floods
- ICMP floods (Internet Control Message Protocol)

UDP Floods

- Random ports on a server are flooded with UDP packets, causing the server to repeatedly check for and respond to non-existent applications at the ports.

- As a result, the system is unable to respond to legitimate applications.

ICMP Floods

- A server is flooded with ICMP echo requests from multiple spoofed IP addresses.
- As the targeted server processes and replies to these phony requests, it is eventually overloaded and unable to process valid ICMP echo requests.

Application – layer attack

- The goal of an application layer attack is to exhaust resources by consuming too much.
- They target the layer that manages HTTP and SMTP communication.
- They target web application packets in order to disrupt the transmission of data between hosts.
- They attack on apache ,windows web servor , as they are more vulnerable.

Application – layer attack

- These type of attacks are more sophisticated and are gaining in popularity than other types of DDoS attacks.

- For example:- an HTTP Flood – the most common application-layer attack – uses botnets to force a target to expend an excessive amount of resources when responding to a HTTP request

Application – layer attack

- HTTP floods and other application-layer DDoS attacks mimic human-user behavior making them much more difficult to detect than other types of attacks.

- Web based email apps, WordPress, Joomla, and forum software are good examples of application specific targets.

Protocol attack

- Protocol attacks target the connection state tables in firewalls, web application servers, and other infrastructure components.

- One of the most common state-exhaustion attacks was the ping of death, in which a 65,536-byte ping packet is defragmented and sent to a target server as fast as possible.

Protocol attack

- Once the target reassembles the large packet, a buffer overload typically occurs.
- In the likely scenario that the target attempts to respond to the pings, even more bandwidth is consumed, eventually causing the targeted system to crash.

DDoS Attack

WE ARE ANONYMOUS.
WE ARE LEGION.
WE DO NOT FORGIVE.
WE DO NOT FORGET.
EXPECT US.

DDoS Attack

- DDoS attacks are the single largest threat to our Internet and the Internet of Things.

- The more our world becomes connected and dependent on the Internet, the more opportunities to get exploited by these types of attack.

FACTS

- There was a 180% percent increase in the total number of DDoS attacks in 2016 compared to 2015.
- The online gaming sector is currently the most susceptible to attack, accounting for 50% of all DDoS attacks.
- Software and technology companies -25%
- Internet and telecoms companies - 5%

of the total attack.

Famous Attack

- 3 Most Famous DDoS Attacks

I. Scientologist Church Gets Hit Hard By Anonymous!

II. Hong Kong's Democracy Movement Attack

III. The New Year Attack !

IV. DDoS in India

Scientologist Church

- This attack took place on January 8, 2008 .
- It was attacked by hacker group Anonymous.
- The DDoS attack was meant to be a protest against the Church of Scientology’s philosophies and practices.
- The program was able to shut down the Scientologist church website momentarily.
- The program that was deployed was used to fight for Wikileaks.

Hong Kong's Democracy Attack

- It started in June 2014, in Hong Kong to bring destruction to the Chinese government . This movement is called Occupy Central.
- Occupy Central used this DDoS attack against the Chinese government because they wanted a one man one vote system when electing officials to represent political office.
- This all led Occupy Central to push their DDoS attack forward and brought down a major political website.

The New Year Attack

- It took place on December 31,2015.
- New World Hacking took responsibly for this huge DDoS attack.
- They were capable of disrupting BBC’s global website, along with Donald Trumps website as well.
- The tool that was used to deploy these attacks is called BangStresser.

The DDoS Attack in India

- It took place on November ,2016.
- It was one of the biggest attack ever done on an ISP.
- The attack was of a huge magnitude of 200 gigabytes per second.
- This is the reason behind the recent slowing down of the internet experienced by users around Mumbai.
- An FIR was filed against the DDoS attack with the Mumbai police.

SYMPTOMS

The United States Computer Emergency Readiness Team(US-CERT) has identified symptoms of a denial-of-service attack to include:

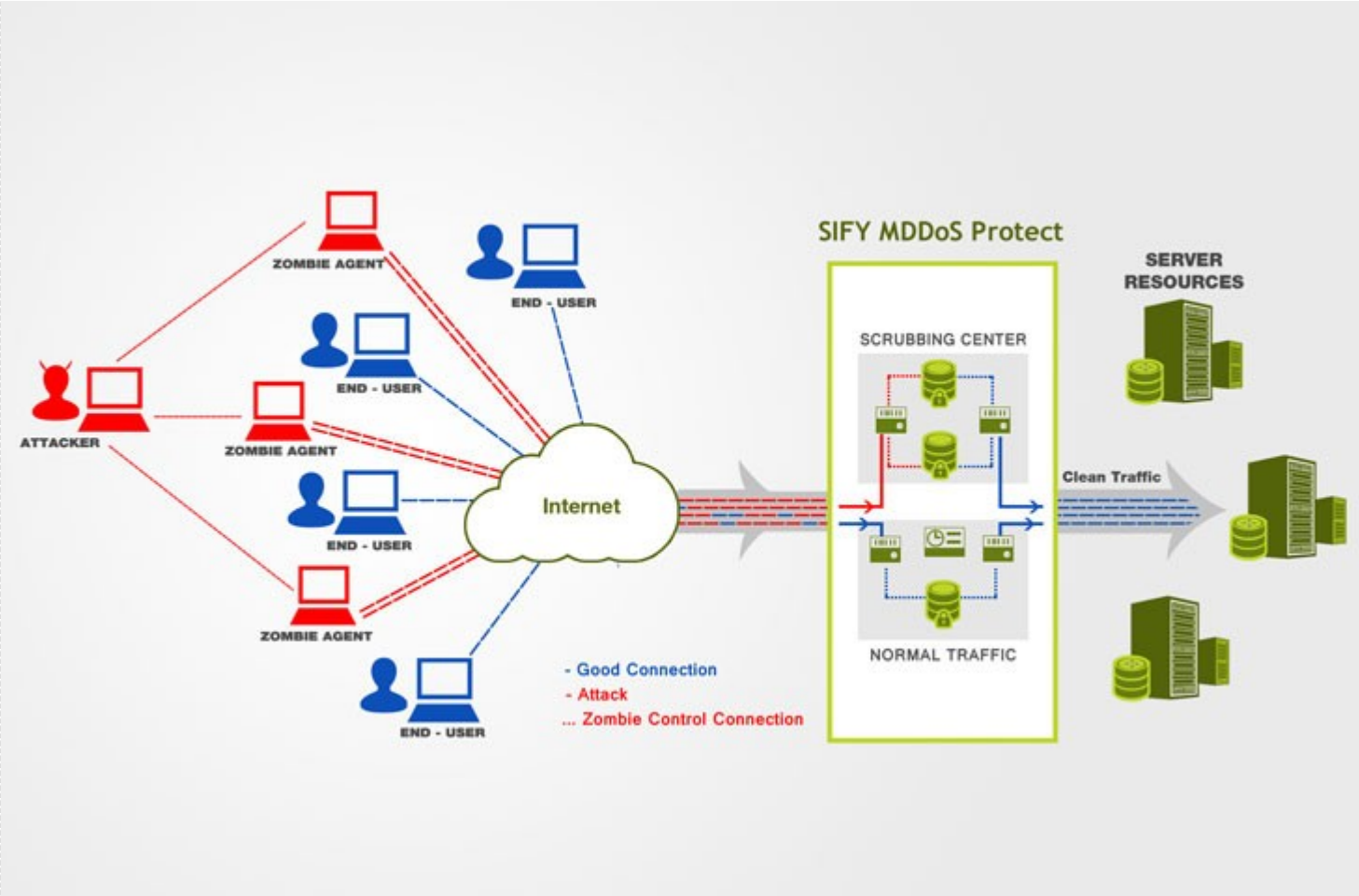
- unusually slow network performance
- unavailability of a particular web site
- inability to access any web site
- dramatic increase in the number of spam emails received (this type of DoS attack is considered an e-mail bomb).

DDoS Mitigation

DDoS Mitigation

- DDoS mitigation is a set of techniques or tools for resisting the impact of DDoS attacks on networks attached to the Internet by protecting the target and relay networks.
- DDoS mitigation also requires identifying incoming traffic to separate human traffic from human-like bots and hijacked web browsers.
- The process is done by comparing signatures and examining different attributes of the traffic, including IP addresses, cookie variations, HTTP headers, and JavaScript footprints.

DDoS Mitigation



DDoS Mitigation

- Best practices for DDoS mitigation include having both anti-DDoS technology and anti-DDoS emergency response services such as Incapsula, Akamai, CloudFlare or Radware.

- DDoS mitigation is also available through cloud-based providers.
- User must install anti-virus.
- User must install firewall.

DDoS Myths

- Myths:

Enterprises believe they are fully protected with only cloud based DDoS mitigation.

- Facts:

Cloud based DDoS mitigation only protects against large, volumetric attacks, and fails to provide adequate protection against low and slow application layer attacks

DDoS Myths

- Myths:

We will not become a target. Our business is too small.

- Facts:

DDoS attacks do not discriminate. Any organization, big or small, is in danger or experiencing the risks associated with a DDoS attack.

DDoS Myths

- Myths:

My Internet Service Provider (ISP) is protecting me from DDoS attacks.

- Facts:

ISP's lack the ability to detect, analyze and mitigate DDoS attacks and other cyber threats

THANK YOU !